UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/795,929	03/08/2004	Leo M. Pedlow JR.	SNY-T5718.02	1819

24337 7590 05/27/2009

MILLER PATENT SERVICES
2500 DOCKERY LANE
RALEIGH, NC 27606

EXAMINER	
JOHNSON, CARLTON	

ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
05/27/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/795,929	PEDLOW ET AL.	
	Examiner	Art Unit	
	CARLTON V. JOHNSON	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 February 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-57* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-57* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responding to application amendments filed on 2-12-2009.

2. Claims **1 - 57** are pending. Claims **1, 9, 16, 23, 29, 35, 41, 47, 52** have been amended. Claims **1, 9, 16, 23, 29, 35, 41, 47, 52** are independent. This application was filed on **3-8-2004**.

Response to Arguments

3. Applicant's arguments have been fully considered but they are not persuasive.

3.1 Applicant argues that the referenced prior art does not disclose, *encryption keys being distinct from keys supplied by and periodically changed by the conditional access management system" (see Remarks Pages 18, 19); default encryption keys (see Remarks Pages 20).*

Bestler prior art discloses encryption processing being linked to communications operating successfully or communications failure. Bestler prior art discloses that after being successfully polled, the head-end downloads a new session key to the corresponding subscriber terminal. When terminal cannot be polled or communications cannot be established, then communication failure has occurred. (see Bestler col. 5, lines 14-19: if the subscriber terminal cannot be polled, then a communications failure has occurred and the subscriber terminal cannot receive the new session key) Bestler prior art discloses that the previous session key are used for decrypting program content in the event of a communications failure.

In the event of communication failure, why are the already transferred keys lost? *(see Remarks Page 18)* Applicant has not given any indicated why this situation must occur.

Yonge prior art discloses default encryption information such as default encryption keys. (see Yonge col 6, lines 27-30: control station; end device such as host computer, cable modem); col. 33, lines 7-17: each station has a unique default key; default is used to allow secure communications between the stations)

There is no disclosure that the active encryption keys are distinct and separate from default encryption key. There is no disclosure that the default encryption keys can only be used in the event of communication failure. The Yonge prior art discloses default keys stored in the prior art invention. *(see Remarks Page 19)*

There does not appear to be a claim limitation to *"always assure"* encryption of content. The claim limitation enables content encryption in the event of communication failure. *(see Remarks Page 20)*

The Dasari prior art was not used in the current Office Action rejection and has been removed. *(see Remarks Page 19)*

Maillard prior art discloses a conditional access system. (see Maillard col. 6, lines 36-42: conditional access system (conditional access management system)) Bestler prior art discloses a set of encryption keys used in the event of communications failure. (see Bestler col. 2, lines 54-56: default encryption key) Furthermore, Bestler prior art

discloses that audio/video content (program content) and control information are encrypted using encryption keys (session key 1 and key 2). (see Bestler col. 5, lines 32-35: if authorized for program defined by accompanying program tag, enable to operate their unscramble apparatus to unscramble (decrypt) the program (unscramble the content))

Claim Rejections - 35 USC § 112

4. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

5. Claims **1, 9, 16, 23, 29, 35, 41, 47, 52** are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. For claims 1, 9, 16, 23, 29, 35, 41, 47, 52 there is no disclosure for the claims limitation: "the default encryption key being distinct from keys supplied by the conditional access management system". There does not appear to be support for the limitation that the default encryption keys are distinct and separate from the encryption keys used during "normal" operation of the conditional access system.

Appropriate correction required.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims **1 - 57** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Maillard et al.** (US Patent No. **6,466,671**) in view of **Bestler et al.** (US Patent No. **4,995,080**) and further in view of **Yonge, III et al.** (US patent No. **6,671,284**).

With Regards to Claim 1, Maillard discloses an apparatus for default encryption of content for distribution, comprising:

a) a conditional access encryption system that uses encryption code words as encryption keys; (see Maillard col. 6, lines 18-22; col. 6, lines 36-42: access system for management of cable functions, conditional access (CA) module (conditional access system))

Furthermore, Maillard discloses a conditional access management system that communicates with and manages the conditional access encryption system; (see Maillard col. 6, lines 36-42: conditional access system (conditional access management system))

Furthermore, Maillard discloses a memory storing encryption information for use by

the conditional access system to encrypt certain content in which said communication failure results in the termination of current encryption activity. (see Maillard col. 1, lines 33-34; col. 6, lines 59-62: memory for encryption keys storage)

Maillard does not specifically disclose encrypting upon a communication failure. However, Bestler discloses the following:

b) provides the encryption keys to the encryption system and periodically changes the encryption keys; (Bestler col. 5, lines 1-5: periodically changing sessions keys; col. 5, lines 14-15: data packets are encrypted with sessions keys)

c) keys periodically changed by the conditional access management system, which said communication failure results in an inability for the conditional access management system to provide the encryption keys to the conditional access encryption system which would otherwise result in the audio/video content being distributed unencrypted and encrypting content upon a communication failure. (see Bestler col. 3, lines 1-6; col. 5, lines 19-22; col. 5, lines 37-39; col. 5, lines 60-63: encryption information utilized for decryption during communications failure; col. 5, lines 1-5: periodically changing sessions keys; col. 5, lines 14-15: data packets are encrypted with sessions keys)

It would have been obvious to one of ordinary skill in the art to modify Maillard to encrypt content upon a communication failure as taught by Bestler. One of ordinary skill in the art would have been motivated to employ the teachings of Bestler for a novel and improved method to operate a pay television (cable system)

and permit a subscriber to self-authorize his equipment to unscramble pay per view programs. (see Bestler col. 1, lines 28-32)

Furthermore, Yonge specifically discloses default encryption information, the default encryption key being distinct from keys supplied for encryption. (see Yonge col 6, lines 27-30: control station; end device such as host computer, cable modem); col. 33, lines 7-17: each station has a unique default key; default key used to allow secure communications between stations)

It would have been obvious to one of ordinary skill in the art to modify Maillard for default encryption information as taught by Yonge. One of ordinary skill in the art would have been motivated to employ the teachings of Yonge to ensure efficient station-to-station dialog or Quality of Service (QoS) requirements. (see Yonge col. 1, lines 37-40)

With Regards to Claims 2, 10, 18, 25, 31, 37, Maillard discloses the apparatus of claims 1, 9, 16, 23, 29, 35, wherein the default encryption information comprises default encryption keys. (see Maillard col. 1, lines 33-37; col. 6, lines 59-62; col. 6, lines 55-58: encryption information (keys) for content encryption, stored)

With Regards to Claims 3, 11, 19, 26, 32, 38, Maillard discloses the apparatus of claims 2, 10, 18, 25, 31, 37, wherein the default encryption keys are unique for each of a plurality of channels. (see Maillard col. 1, lines 64 - col. 2, line 1; col. 4, lines 49-54: encryption key unique for each channel)

With Regards to Claim 4, Maillard discloses the apparatus of claim 1, further comprising a control computer that initializes the configuration memory with the default encryption information. (see Maillard col. 1, lines 33-37; col. 6, lines 59-62; col. 1, line 61 - col. 2, line 1: memory, setup configuration information (encryption information))

With Regards to Claims 5, 12, 20, 27, 33, 39, Maillard discloses the apparatus of claims 1, 9, 16, 23, 29, 35, wherein the configuration memory comprises a non-volatile memory. (see Maillard col. 1, lines 33-37; col. 6, lines 59-62: non-volatile memory utilized for operational (configuration) information)

With Regards to Claims 6, 13, Maillard discloses the apparatus of claims 1, 9, wherein the content is encrypted with the encryption information between the conditional access management system and the conditional access system. (see Maillard col. 6, lines 45-49; col. 7, lines 46-49; col. 6, lines 55-58: content encrypted, pre-setup configuration information (encryption keys))

Maillard does not specifically disclose encryption during communication failure. However, Bestler discloses content is encrypted with default encryption information when communication failure occurs. (see Bestler col. 3, lines 1-6; col. 5, lines 19-22; col. 5, lines 37-39; col. 5, lines 60-63: encryption information (default) utilized for decryption during communications failure)

Motivation to modify Maillard as taught by Bestler is stated in Claim 1 above.

With Regards to Claims 7, 14, Maillard discloses the apparatus of claims 1, 9, wherein the content is encrypted with default encryption information between the conditional access management system and the conditional access encryption system. (see Maillard col. 6, lines 45-49; col. 7, lines 46-49; col. 6, lines 55-58: encryption of content utilizing encryption keys)

Maillard does not specifically disclose encryption during communication failure. However, Bestler discloses content is encrypted when communication cannot be established. (see Bestler col. 3, lines 1-6; col. 5, lines 19-22; col. 5, lines 37-39; col. 5, lines 60-63: encryption information utilized for decryption during communications failure)

Motivation to modify Maillard as taught by Bestler is stated in Claim 1 above.

With Regards to Claims 8, 15, 21, Maillard discloses the apparatus according to claims 1, 9, 16, wherein the conditional access system provides selective encryption of the content. (see Maillard col. 6, lines 45-49; col. 7, lines 46-49; col. 6, lines 55-58: selective encryption (encryption of partial content))

With Regards to Claim 9, Maillard discloses an apparatus for default encryption, comprising:

a) conditional access system; (see Maillard col. 6, lines 18-22; col. 6, lines 36-42: access system for management of cable functions, conditional access (CA) module (conditional access system))

Furthermore, Maillard discloses the following:

b) means for encrypting content in the conditional access system that uses encryption code words as encryption keys; (see Maillard col. 7, lines 54-58; col. 7, line 66 - col. 8, line 4: content (encrypted) distributed over communications medium; col. 6, lines 59-65; col. 9, lines 27-31; col. 25, lines 37-39: software implementation, means; col. 7, lines 5-15: scramble (encrypt) content); specification page 3, line 1 defines code words to be equivalent to encryption keys)

d) means for communicating between the managing means and the encrypting means; (see Maillard col. 10, lines 10-16; col. 12, lines 36-45: command processing, conditional access system; col. 6, lines 59-65; col. 9, lines 27-31; col. 25, lines 37-39: software implementation, means)

f) means for configuring the storing means with the encryption information. (see Maillard col. 1, line 61 - col. 2, line 1: configure encryption information; col. 6, lines 59-65; col. 9, lines 27-31; col. 25, lines 37-39: software implementation, means)

Furthermore, Maillard discloses means for storing encryption information for the conditional access system for use by the conditional access system to encrypt certain audio/video content in which said communications failure results in the termination of current encryption activity. (see Maillard col. 1, lines 33-34; col. 1, line 61 - col. 2, line 1: storage configuration (encryption) information; col. 4, lines 28-29: receive and decrypt video and/or audio signals; col. 7, lines 5-15:

scramble (encrypt) content)

Furthermore, Maillard discloses means for managing conditional access system, (see Maillard col. 6, lines 36-42: conditional access system (conditional access management system); col. 6, lines 59-65; col. 9, lines 27-31; col. 25, lines 37-39: software implementation, means)

Maillard does not specifically disclose encryption during communication failure. However, Bestler discloses the following:

c) the means for managing provides the encryption keys to the means for encrypting and periodically changes the encryption keys; (Bestler col. 5, lines 1-5: periodically changing sessions keys; col. 5, lines 14-15: data packets are encrypted with sessions keys)

e) a communication failure, an inability for the managing means to provide the means for encryption keys to the means for encrypting which would otherwise result in the audio/video content being distributed unencrypted and periodically changed by the means for managing; (see Bestler col. 3, lines 1-6; col. 5, lines 19-22; col. 5, lines 37-39; col. 5, lines 60-63: encryption information (default) utilized for decryption during communications failure; col. 5, lines 1-5: periodically changing sessions keys; col. 5, lines 14-15: data packets are encrypted with sessions keys)

Motivation to modify Maillard as taught by Bestler is stated in Claim 1 above.

Furthermore, Yonge discloses default encryption information and default encryption

key being distinct from keys supplied. (see Yonge col 6, lines 27-30: control station; end device such as host computer, cable modem); col. 33, lines 7-17: each station has a unique default key; default is used to allow secure communications between the stations)

Motivation to modify Maillard as taught by Yonge is stated in Claim 1 above.

With Regards to Claim 16, Maillard discloses a method of default encryption of audio/video content for distribution, comprising:

a) initializing a default configuration memory with default encryption information; (see Maillard col. 1, lines 33-34; col. 6, lines 59-62: memory; col. 1, line 61 - col. 2, line 1: initialize memory; col. 23, lines 8-14: transfer (initialize) with configuration (encryption) information)

Furthermore, Maillard discloses the following:

b) communicating with a conditional access management system to retrieve active encryption information for a conditional access system; (see Maillard col. 23, lines 8-14: receive (transfer) encryption keys, normal operation)

c) encrypting content for distribution with the active encryption information; distributing the content encrypted with active encryption information; (see Maillard col. 6, lines 45-49; col. 7, lines 46-49: content encrypted with encryption keys)

e) distributing the audio/video content encrypted with the encryption information. (see Maillard col. 7, lines 54-58; col. 7, line 66 - col. 8, line 4: content

(encrypted) distributed over communications medium; col. 4, lines 28-29: receive and decrypt (distribute) video and/or audio signals)

f) encrypting the audio/video content with the encryption information; (see Maillard col. 6, lines 45-49; col. 7, lines 46-49: encrypt content utilizing encryption keys; col. 7, lines 5-15: scramble (encrypt) content))

Maillard does not specifically disclose communication failure.

However, Bestler discloses the following when communication failure occurs:

d) encryption information and reading the encryption information from the configuration memory in which said communication failure results in an inability for the conditional access management system to provide updated active encryption information to support the encrypting which would otherwise result in the audio/video content being distributed unencrypted; (see Bestler col. 3, lines 1-6; col. 5, lines 19-22; col. 5, lines 37-39; col. 5, lines 60-63: encryption information utilized for decryption during communications failure; col. 5, lines 1-5: periodically changing sessions keys; col. 5, lines 14-15: data packets are encrypted with sessions keys)

Motivation to modify Maillard as taught by Bestler is stated in Claim 1 above.

Furthermore, Yonge discloses default encryption information, the default encryption being distinct from active encryption information supplied. (see Yonge col 6, lines 27-30: control station; end device such as host computer, cable modem; col. 33, lines 7-17: each station has a unique default key; default used to allow secure

communications between stations)

Motivation to modify Maillard as taught by Yonge is stated in Claim 1 above.

With Regards to Claim 17, Maillard discloses the method of claim 16, further comprising:

communication restored between the conditional access management system and the conditional access system:

a) communicating with the conditional access management system to retrieve active encryption information for the conditional access system; (see Maillard col. 23, lines 8-14: retrieve configuration (encryption) information, normal operation)

Furthermore, Maillard discloses the following:

b) encrypting the audio/video content for distribution with the active encryption information; (see Maillard col. 6, lines 45-49; col. 7, lines 46-49: encrypt content utilizing encryption information; col. 4, lines 28-29: receive and decrypt video and/or audio signals)

c) distributing the audio/video content encrypted with active encryption information. (see Maillard col. 7, lines 54-58; col. 7, line 66 - col. 8, line 4: content (encrypted) distributed over communications medium)

With Regards to Claims 22, 28, 34, 40, Maillard discloses a computer readable medium storing instructions which, when executed on a programmed processor, carry

out the process according to claims 16, 23, 29, 35. (see Maillard col. 6, lines 59-65; col. 9, lines 27-31; col. 25, lines 37-39: software implementation)

With Regards to Claim 23, Maillard discloses a method of default encryption of content for distribution, comprising:

a) initializing a default configuration memory with default encryption information; (see Maillard col. 1, lines 33-34; col. 6, lines 59-62: memory; col. 1, line 61 - col. 2, line 1: initialize memory; col. 23, lines 8-14: transfer (initialize) with configuration (encryption) information)

Furthermore, Maillard discloses the following:

b) attempting to communicate with a conditional access management system to retrieve active encryption information for a conditional access system; (see Maillard col. 10, lines 10-16; col. 12, lines 36-45: command processing, conditional access system)

e) encrypting the audio/video content with the default encryption information; (see Maillard col. 6, lines 45-49; col. 7, lines 46-49; col. 6, lines 55-58: encrypt content with encryption keys; col. 4, lines 28-29: receive and decrypt video and/or audio signals; col. 7, lines 5-15: scramble (encrypt) content)) and

f) distributing the audio/video content encrypted with the default encryption information. (see Maillard col. 7, lines 54-58; col. 7, line 66 - col. 8, line 4: content (encrypted) distributed over communications medium)

Maillard does not specifically disclose communication cannot be established.

However, Bestler discloses wherein communication cannot be established:

d) reading the encryption information from the configuration memory in which said communication failure results in an inability for the conditional access management system to provide the active encryption information to the conditional access encryption system which would otherwise result in the audio/video content being distributed unencrypted; (see Bestler col. 3, lines 1-6; col. 5, lines 19-22; col. 5, lines 37-39; col. 5, lines 60-63: encryption information (default) utilized for decryption during communications failure; col. 5, lines 1-5: periodically changing sessions keys; col. 5, lines 14-15: data packets are encrypted with sessions keys))

Motivation to modify Maillard as taught by Bestler is stated in Claim 1 above.

Furthermore, Yonge discloses default encryption information, the default encryption information being distinct active encryption information supplied by the conditional access management system. (see Yonge col 6, lines 27-30: control station; end device such as host computer, cable modem; col. 33, lines 7-17: each station has a unique default key; default is used to allow secure communications between the stations)

Motivation to modify Maillard as taught by Yonge is stated in Claim 1 above.

With Regards to Claim 24, Maillard discloses the method of claim 23, further comprising:

communication achieved between the conditional access management system and

the conditional access system:

b) receiving active encryption information for the audio/video content for distribution in the conditional access system; (see Maillard col. 23, lines 8-14;: receive (transfer) encryption keys, normal operation; col. 4, lines 28-29: receive and decrypt video and/or audio signals)

Furthermore, Maillard discloses the following:

c) encrypting the content with the active encryption information; (see Maillard col. 6, lines 45-49; col. 7, lines 46-49; col. 6, lines 55-58: content encrypted with encryption keys) and

d) distributing the content encrypted with active encryption information. (see Maillard (see Maillard col. 7, lines 54-58; col. 7, line 66 - col. 8, line 4: content (encrypted) distributed over communications medium)

With Regards to Claims 29, 35, Maillard discloses a method of default encryption of audio/video content for distribution, comprising:

a) initializing a default configuration memory with default encryption information; (see Maillard col. 1, lines 33-34; col. 6, lines 59-62; col. 1, line 61 - col. 2, line 1: configuration (encryption) information stored in memory; col. 4, lines 28-29: receive and decrypt video and/or audio signals)

Furthermore, Maillard discloses the following:

b) communicating with a conditional access management system to retrieve active encryption information for the content for distribution in a conditional access

system; (see Maillard col. 23, lines 8-14: transfer configuration (encryption) information)

c) encrypting the audio/video content with the active encryption information; distributing the audio/video content encrypted with active encryption information; (see Maillard col. 6, lines 45-49; col. 7, lines 46-49; col. 6, lines 55-58: content (encrypted) and distributed; col. 7, lines 5-15: scramble (encrypt) content))

d) signaling all set-top boxes within the conditional access system instructing them to use the active encryption information; (see Maillard col. 10, lines 10-16; col. 12, lines 36-45: command process, conditional access system; encryption keys sent to set top box)

f) encrypting the audio/video content with the default encryption information; (see Maillard col. 6, lines 45-49; col. 7, lines 46-49; col. 6, lines 55-58: content encrypted with default encryption keys)

g) signaling all set-top boxes within the conditional access system instructing them to use the default encryption information; (see Maillard col. 10, lines 10-16; col. 12, lines 36-45: command processing, conditional access system; col. 15, line 63 - col. 16, line 3: no communications for some set-top boxes, still connected set top boxes configure using encryption keys) and

h) distributing the audio/video content encrypted with the default encryption information. (see Maillard col. 7, lines 54-58; col. 7, line 66 - col. 8, line 4: distributed content for usage by both connected set-top boxes and disconnected set-top boxes)

Maillard does not specifically disclose communication failure.

However, Bestler discloses the following during communication failure:

e) reading the encryption information from the configuration memory said communication failure results in an inability for the conditional access management system to provide the active encryption information to the conditional access encryption system which would otherwise result in the audio/video content being distributed unencrypted; (see Bestler col. 3, lines 1-6; col. 5, lines 19-22; col. 5, lines 37-39; col. 5, lines 60-63: encryption information utilized for decryption during communications failure; col. 5, lines 1-5: periodically changing sessions keys; col. 5, lines 14-15: data packets are encrypted with sessions keys))

Motivation to modify Maillard as taught by Bestler is stated in Claim 1 above.

Furthermore, Yonge discloses default encryption information, the default encryption information being distinct from active encryption information supplied by the conditional access management system. (see Yonge col 6, lines 27-30: control station; end device such as host computer, cable modem; col. 33, lines 7-17: each station has a unique default key; default is used to allow secure communications between stations)

Motivation to modify Maillard as taught by Yonge is stated in Claim 1 above.

With Regards to Claims 30, 36, Maillard discloses the method of claims 29, 35, further

comprising:

communication restored/achieved between the conditional access management system and the conditional access system:

a) receiving active encryption information for the audio/video content for distribution in the conditional access system; (see Maillard col. 7, lines 54-58; col. 7, line 66 - col. 8, line 4: encryption information transferred/received, normal operation)

Furthermore, Maillard discloses the following:

b) encrypting the audio/video content with the active encryption information; (see Maillard col. 6, lines 45-49; col. 7, lines 46-49; col. 6, lines 55-58: content encrypted with encryption keys)

c) signaling all set-top boxes within the conditional access system instructing them to use the active encryption information; (see Maillard col. 10, lines 10-16; col. 12, lines 36-45: command processing by conditional access system; col. 1, line 61 - col. 2, line 1: configure encryption information) and

d) distributing the audio/video content encrypted with active encryption information. (see Maillard col. 7, lines 54-58; col. 7, line 66 - col. 8, line 4: distribute encrypted content)

With Regards to Claim 41, Maillard discloses an apparatus for default decryption of audio/video content, comprising:

a) a receiver conditional access system that provides decryption functions; (see Maillard col. 6 , lines 18-22; col. 6, lines 36-42: access system for management

of cable functions, conditional access (CA) module (conditional access system))

Furthermore, Maillard discloses the following:

e) memory also storing decryption key for use to decrypt the audio/video content when the conditional access system receives signaling instructing it to use the decryption key instead of the alternate decryption keys. (see Maillard col. 10, lines 10-16; col. 12, lines 36-45: command processing, conditional access system; col. 1, lines 33-34; col. 6, lines 59-62: memory, storage configuration information)

Furthermore, Maillard discloses a memory storing decryption keys used by decrypters. (see Maillard col. 1, lines 33-34; col. 6, lines 59-62: memory for encryption keys storage)

Maillard does not specifically disclose an alternate decryption engine and storing alternate decryption keys.

However, Bestler discloses the following:

b) an odd and even decryption engine; an odd decryption engine; (see Bestler col. 5, lines 32-35: encryption keys alternatively used for encryption (scrambling); two sets of keys used for encryption/decryption; session key 1 and session key 2 for encryption of content (program content))

c) odd and even decryption keys for use by the odd and even decryption engine; (see Bestler col. 5, lines 32-35: encryption keys alternatively used for encryption (scrambling))

f) wherein, such signaling instruction is received when a communication failure at an audio/video content provider would otherwise permit content to be provided without benefit of encryption for decryption using the odd and even decryption keys. (see Bestler col. 3, lines 1-6; col. 5, lines 19-22; col. 5, lines 37-39; col. 5, lines 60-63: encryption information (default) utilized for decryption during communications failure)

Motivation to modify Maillard as taught by Bestler is stated in Claim 1 above.

With Regards to Claims 42, 48, 54, Maillard discloses the apparatus of claims 41, 47, 52, wherein the default decryption information comprises default decryption keys. (see Maillard col. 1, line 61 - col. 2, line 1: encryption/decryption information (keys) for content encryption)

With Regards to Claims 43, 49, 55, Maillard discloses the apparatus of claims 42, 48, 54, wherein the default decryption keys are unique for each of a plurality of channels. (see Maillard col. 1, line 61 - col. 2, line 1; col. 4, lines 49-54: encryption/decryption key unique for each channel)

With Regards to Claim 44, Maillard discloses the apparatus of claim 41, wherein, when signaled to initialize the default decryption key, the conditional access system initializes the memory with default encryption information received with the signaling. (see Maillard col. 1, line 61 - col. 2, line 1: configuration information processed)

With Regards to Claims 45, 50, 56, Maillard discloses the apparatus of claims 41, 47, 52, wherein the configuration memory comprises a non-volatile memory. (see Maillard col. 1, lines 33-34; col. 6, lines 59-62: non-volatile memory utilized for operational (configuration) information)

With Regards to Claim 46, Maillard discloses the apparatus of claim 41, wherein the content is decrypted with the default decryption key upon reception of signaling instructing the conditional access system to use the default decryption key. (see Maillard col. 1, line 61 - col. 2, line 1: communication restored, process configuration (encryption) information)

With Regards to Claim 47, Maillard discloses an apparatus for default decryption of audio/video content, comprising:

a) means for receiving audio/video content in a conditional access system that provides decryption functions; (see Maillard col. 7, lines 54-58; col. 7, line 66 - col. 8, line 4: received (encrypted) content; col. 6, lines 59-65; col. 9, lines 27-31; col. 25, lines 37-39: software implementation, means)

Furthermore, Maillard discloses the following:

d) means for receiving signaling in the conditional access system; (see Maillard col. 6, lines 18-22; col. 6, lines 36-42: conditional access system; col. 10, lines 10-16; col. 12, lines 36-45: command processing; signaling for conditional access

system; col. 6, lines 59-65; col. 9, lines 27-31; col. 25, lines 37-39: software implementation, means)

f) means for configuring the storing means with the default decryption information. (see Maillard col. 1, line 61 - col. 2, line 1: configure encryption information; col. 6, lines 59-65; col. 9, lines 27-31; col. 25, lines 37-39: software implementation, means)

Furthermore, Maillard discloses a memory storing decryption keys used by decryption engines. (see Maillard col. 1, lines 33-34; col. 6, lines 59-62: memory for encryption keys storage)

Furthermore, Maillard discloses means for storing decryption information for audio/video content received in the conditional access system for use to decrypt the audio/video content when the conditional access system receives signaling instructing it to use the decryption information. (see Maillard col. 1, lines 33-34; col. 6, lines 59-62: storage configuration information in memory; col. 6, lines 59-65; col. 9, lines 27-31; col. 25, lines 37-39: software implementation, means)

Maillard does not specifically disclose an alternate decryption engine and storing alternate decryption keys.

However, Bestler discloses the following:

b) an odd and even decryption engine; an odd decryption engine; (see Bestler col. 5, lines 32-35: encryption keys alternatively used for encryption (scrambling); two sets of keys used for encryption/decryption; session key 1 and session key 2 for

encryption of content (program content))

c) odd and even decryption keys for use by the an odd and even decryption engines; (see Bestler col. 5, lines 32-35: encryption keys alternatively used for encryption (scrambling))

e) odd and even decryption keys wherein such signaling instruction is received when a communication failure at an audio/video content provider would otherwise permit content to be provided without benefit of encryption for decryption using the alternate decryption keys; (see Bestler col. 5, lines 32-35: encryption keys alternatively used for encryption (scrambling))

Motivation to modify Maillard as taught by Bestler is stated in Claim 1 above.

With Regards to Claim 51, Maillard discloses the apparatus of claim 47, wherein the content is decrypted with the default decryption information upon reception of signaling instructing the conditional access system to use the default decryption information. (see Maillard col. 10, lines 10-16; col. 12, lines 36-45: command processing, conditional access system; col. 1, line 61 - col. 2, line 1: utilize configuration information, encryption keys)

With Regards to Claim 52, Maillard discloses a method of default decryption of audio/video content, comprising:

b) receiving signaling instructing storage of decryption information for audio/video content in a conditional access system; (see Maillard col. 10, lines 10-16; col.

12, lines 36-45: command processing, conditional access system)

Furthermore, Maillard discloses the following:

c) receiving decryption information for use to decrypt the audio/video content when the conditional access system receives signaling instructing it to use the default decryption information; (see Maillard col. 10, lines 10-16; col. 12, lines 36-45: command processing, conditional access system; col. 23, lines 8-14: receive configuration information)

d) initializing a default configuration memory with the decryption information; (see Maillard col. 1, lines 33-34; col. 6, lines 59-62; col. 1, line 61 – col. 2, line 1: memory, initialized (storage) configuration information)

e) receiving active decryption information with audio/video content in the conditional access system; (see Maillard col. 23, lines 8-14: receive configuration information)

signaling reception instructs use of the decryption information for the conditional access system:

g) reading the decryption information for the audio/video content from the default configuration memory; (see Maillard col. 23, lines 8-14; col. 1, line 61 - col. 2, line 1: configure encryption information, normal operation) and

h) decrypting audio/video content with the decryption information. (see Maillard col. 8, lines 17-22: decrypt content)

Furthermore, Maillard discloses decrypting selected channels. (see Maillard col. 8, lines 17-22: decrypt content)

Maillard does not specifically disclose even and odd decryption information. However, Bestler discloses the following encryption information:

a) receiving audio/video content in a conditional access system that provides decryption functions, said audio/video content normally being decrypted using an even decryption engine and an odd decryption engine operating. (see Bestler col. 5, lines 32-35: encryption keys alternatively used for encryption (scrambling); two sets of keys used for encryption/decryption; session key 1 and session key 2 for encryption of content (program content))

f) odd and even decryption engines using the odd and even decryption keys; (see Bestler col. 5, lines 32-35: encryption keys alternatively used for encryption (scrambling))

i) wherein, such signaling reception instructs use of the default decryption information when a communication failure at an audio/video content provider would otherwise permit content to be provided without benefit of encryption for decryption using the odd or even decryption keys. (see Bestler col. 3, lines 1-6; col. 5, lines 19-22; col. 5, lines 37-39; col. 5, lines 60-63: encryption information (default) utilized for decryption during communications failure; col. 5, lines 32-35: encryption keys alternatively used for encryption (scrambling))

Motivation to modify Maillard as taught by Bestler is stated in Claim 1 above.

With Regards to Claim 53, Maillard discloses the method of claim 52, further comprising: if signaling reception instructs use of active decryption information:

a) receiving active decryption information with the content in the conditional access system; (see Maillard col. 23, lines 8-14: receive configuration information)

Furthermore, Maillard discloses the following:

b) decrypting content with the active decryption information. (see Maillard col. 8, lines 17-22: decrypt content)

With Regards to Claim 57, Maillard discloses a computer readable medium storing instructions which, when executed on a programmed processor, carry out the process according to claim 52. (see Maillard col. 6, lines 59-65; col. 9, lines 27-31; col. 25, lines 37-39: software implementation)

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carlton V. Johnson whose telephone number is 571-270-1032. The examiner can normally be reached on Monday thru Friday , 8:00 - 5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2436

Carlton V. Johnson
Examiner
Art Unit 2436

CVJ
May 11, 2009